ATTACHMENT B
ITEMS TO BE SEARCHED FOR AND SEIZED

1. Computers, images of child pornography and files containing images of child pornography in any form wherever it may be stored or found including, but not limited to:

   a) Any computer, computer system, and central processing unit; any digital, electronic, optical, or magnetic storage or production device to include, but not limited to, cellular telephones, personal data assistants, internal or external hard or floppy disks and drives, flash memory devices, tape drives and tapes, optical media (CD/DVD), dongles or encryption keys, digital cameras, scanners, gaming consoles; peripheral input/output devices such as keyboards, printers, video display monitors, optical readers; related communications devices such as modems, routers, and network access devices; system documentation, operating logs, and documentation, software, passwords, and instruction manuals; all of which being related to, or used to, visually depict child pornography, contain information pertaining to the interest in child pornography, and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography;

b) Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

c) Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

d) Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

2. Information, correspondence, records, documents or other material pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using a computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

a) Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, web logs ("blogs") and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

b) Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

c) Any and all records, documents, or materials, including any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

d) Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include ISP records, i.e., billing and subscriber records, chat room logs, e-mail messages, web logs, web site postings, and include electronic files in a computer and on other digital data storage mediums;

e) Credit card information including but not limited to bills and payment records;

f) Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;

g) Records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

3. For any computer hard drive or other electronic digital media (hereinafter referred to as "COMPUTER") found to contain information otherwise called for by this warrant:

a) Evidence of who used, owned, or controlled the COMPUTER at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, user names and passwords, documents, and file and web browsing history;

b) Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software;

c) Evidence of the attachment to the COMPUTER of other storage devices, disks, CD-ROMs, DVDs, flash drives or similar containers for electronic evidence;

d) Evidence of the dates and times the COMPUTER was used;

4. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

5. Documentation and manuals that may be necessary to access or conduct an examination of the COMPUTER.

ADDENDUM TO ATTACHMENT B

The government shall make an exact copy of all data and other electronically stored information from the seized data storage devices within ten (10) business days after the warrant is executed. Upon written request by the owner of the seized data storage devices the government shall provide the owner with a copy of any requested data and electronically stored information that does not constitute contraband or instrumentalities of a crime. The government shall provide such copy to the owner within reasonable time after a written request is made. If the government withholds any data or electronically stored information requested by the owner, the government shall identify the data and information withheld and explain why it was not produced. The government and the owner shall negotiate the procedures for providing copies of data and electronically stored information, which may require the owner to provide blank storage media at his or her expense.

(a) The term "data storage devices" refers to computer hard drives, diskettes, CD-ROMS, and other devices which contain data and electronically stored information seized pursuant to the search warrant.

(b) The reasonable time period for providing the owner with a copy of data and electronically stored information includes the time required for the government to analyze the data and information to determine whether they contain contraband or

instrumentalities of a crime. Although the court has not set a specific time period for such production, the government shall provide the owner with a copy of the data and electronically stored information requested as soon as practicable under the existing circumstances.

(c) At the conclusion of the criminal investigation and any related criminal proceedings, the government shall return the seized data storage devices, and any data and information contained thereon, to the owner, except for any data storage devices, data, and information which are contraband or instrumentalities of a crime or which are subject to forfeiture under federal or state law.